

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S2	1	("20050044378").PN.	US-PGPUB; USPAT	OR	OFF	2007/02/09 22:31
S3	34	first adj password same second adj password same third adj password	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 13:19
S4	13	((("4,974,156") or ("5,239,294") or ("5,280,581") or ("5,737,421") or ("5,802,176") or ("5,870,465") or ("5,887,065") or ("5,903,571") or ("5,903,642") or ("5,937,068") or ("6,131,164") or ("6,360,258") or ("6,564,121"))).PN.	US-PGPUB; USPAT	OR	OFF	2007/02/10 19:02
S5	18	first adj password same second adj password same encrypted adj key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 20:09
S6	679	(713/171).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/02/10 20:09
S7	404	(713/171).CCLS.	USPAT	OR	OFF	2007/02/10 21:03
S8	6	((("6,005,939") or ("5,398,285") or ("5,737,419") or ("5,557,678") or ("6,072,876") or ("6,094,721"))).PN.	USPAT	OR	OFF	2007/02/10 20:40
S9	275	(713/171).CCLS.	US-PGPUB	OR	OFF	2007/02/10 21:12
S10	3	security adj module same authorization adj module same password same encrypted adj key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:13
S11	3	authorization adj module same password same encrypted adj key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:13
S12	1	authorization adj server same password same encrypted adj key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:14

EAST Search History

S13	38	password same generat\$3 with encrypted adj key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:22
S14	4736	password same encrypted adj key same decrypt\$3 encrypted adj key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:22
S15	85	password same encrypted adj key same decrypt\$3 with encrypted adj key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:27
S16	0	password same encrypted adj key same decrypt\$3 with encrypted adj key same challenge	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:27
S17	22	encrypted adj key same decrypt\$3 with encrypted adj key same challenge	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:29
S18	856	encrypted same decrypt\$3 same challenge	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:30
S19	8	encrypted adj (nonce value) same decrypt\$3 with encrypted adj (nonce value) same challenge	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:35
S20	0	encrypted near3 (number) same decrypt\$3 with encrypted adj (nonce value) same challenge	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:35

EAST Search History

S21	49	encrypted near3 (number) same decrypt\$3 with encrypted near3 (number) same challenge	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:38
S22	3	encrypted near3 (number) same decrypt\$3 with encrypted near3 (number) same challenge same (smart adj card ic adj card)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:39
S23	24	encrypted near3 (number) same decrypt\$3 with encrypted near3 (number) same challenge same (card)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:44
S24	9	receiv\$3 near3 first adj password with (generat\$3 encrypted adj (key number value nonce random))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/10 21:45
S25	1	("20050044378").PN.	US-PGPUB; USPAT	OR	OFF	2007/02/22 12:53
S26	31	(ic adj card smart adj card smartcard) same (password) same encrypted adj (key id identifier value nonce number)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:40
S27	288	(726/7).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/02/22 15:48
S28	76	("5590199").URPN.	USPAT	OR	ON	2007/02/22 14:40
S29	3	(ic adj card smart adj card smartcard) same (authorized adj user adj list)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:41
S30	769	(ic adj card smart adj card smartcard) same (authorized adj user)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:42

EAST Search History

S31	76	((ic adj card smart adj card smartcard) same (authorized adj user)).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:44
S32	2	((ic adj card smart adj card smartcard) same (user adj list)).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:45
S33	30	((ic adj card smart adj card smartcard) same (user adj list))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:49
S34	393	(ic adj card smart adj card smartcard) with authorized adj user	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:49
S35	176	(ic adj card smart adj card smartcard) with (authorized valid) adj user near4 card	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:54
S36	0	(ic adj card smart adj card smartcard) with (authorized valid) adj user near4 card with passwrod	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:54
S37	12	(ic adj card smart adj card smartcard) with (authorized valid) adj user near4 card with password	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:57
S38	190	(ic adj card smart adj card smartcard) with (multiple near3 users)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/22 14:58
S39	1	("4,928,001").PN.	US-PGPUB; USPAT	OR	OFF	2007/02/22 15:08

EAST Search History

S40	1	("20050050319").PN.	US-PGPUB; USPAT	OR	OFF	2007/02/22 15:08
S41	1331	(726/4).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/02/22 15:48
S42	1	("4928001").PN.	US-PGPUB; USPAT	OR	OFF	2007/02/23 14:42
S43	4	("4650975" "4656342" "4683372" "4736094").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/02/23 14:42
S44	52	("4928001").URPN.	USPAT	OR	ON	2007/02/23 15:05
S45	5	authorized adj user adj list same master adj list	USPAT	OR	ON	2007/02/23 15:06
S46	6	authorized adj user adj list same master adj list	US-PGPUB; USPAT.	OR	ON	2007/02/23 15:13
S47	23	user adj list same master adj list	US-PGPUB; USPAT	OR	ON	2007/02/23 15:14
S48	9	access adj list same master adj list	US-PGPUB; USPAT	OR	ON	2007/02/23 15:18
S49	1	two adj supervisor with (access\$3 authoriz\$3 add\$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/23 16:44
S50	21	two adj administrator with (access\$3 authoriz\$3 add\$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/23 16:41
S51	5	two adj supervisor with (approv\$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/23 16:45
S52	1933	smart adj card with server	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/23 17:22
S53	765	smart adj card near4 server	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/23 17:24

EAST Search History

S54	184	smart adj card near4 server	USPAT	OR	ON	2007/02/23 17:29
S55	12	server same decrypt\$3 with encrypted adj key same authenticat\$3	USPAT	OR	ON	2007/02/23 17:30


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

 Terms used encrypted
key authorization scheme password access

Found 74 of 197,895

Sort results by


[Save results to a Binder](#)
[Try an Advanced Search](#)
[Try this search in The ACM Guide](#)

Display results


[Search Tips](#)
☐ Open results in a new window

Results 1 - 20 of 74

 Result page: [1](#) [2](#) [3](#) [4](#) [next](#)

 Relevance scale ☐ ☐ ☐ ☐ ☐

1 [General storage protection techniques: Securing distributed storage: challenges, techniques, and systems](#)



Vishal Kher, Yongdae Kim

 November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**

Publisher: ACM Press

 Full text available: pdf(294.61 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems. We cover a broad range of the storage security literature, present a critical review of the existing solutions, compare ...

Keywords: authorization, confidentiality, integrity, intrusion detection, privacy

2 [Password Management and Digital Signatures: Delegation of cryptographic servers for capture-resilient devices](#)



Philip MacKenzie, Michael K. Reiter

 November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**

Publisher: ACM Press

 Full text available: pdf(312.90 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

A device that performs private key operations (signatures or decryptions), and whose private key operations are protected by a password, can be immunized against offline dictionary attacks in case of capture by forcing the device to confirm a password guess with a designated remote server in order to perform a private key operation. Recent proposals for achieving this allow untrusted servers and require no server initialization per device. In this paper we extend these proposals to enable dynami ...

3 [Improved proxy re-encryption schemes with applications to secure distributed storage](#)



Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger

 February 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 1

Publisher: ACM Press

Full text available:  pdf(331.59 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called *atomic proxy re-encryption*, in which a semitrusted proxy converts a ciphertext for Alice into a ciphertext for Bob *without* seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. ...

Keywords: Proxy re-encryption, bilinear maps, double decryption, key translation


4 Cryptographic key management



Dahl A. Gerberick

May 1990 **ACM SIGSAC Review**, Volume 8 Issue 2

Publisher: ACM Press

Full text available:  pdf(962.96 KB) Additional Information: [full citation](#), [abstract](#), [index terms](#)

There are two main issues concerning data security on networks; controlling access and the vulnerability of data communication links. A brief introduction to the various techniques which may be applied to these concerns are given in this paper.

5 Distributed PIN verification scheme for improving security of mobile devices

Jian Tang, Vagan Terziyan, Jari Veijalainen

April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2

Publisher: Kluwer Academic Publishers

Full text available:  pdf(298.43 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The main driving force for the rapid acceptance rate of small sized mobile devices is the capability to perform e-commerce transactions at any time and at any place, especially while on the move. There are, however, also weaknesses of this type of e-commerce, often called mobile e-commerce, or m-commerce. Due to their small size and easy portability mobile devices can easily be lost or stolen. Whereas the economic values and privacy threats protected with Personal Identification Numbers (PIN) are ...

Keywords: measure, mobile device, probability, risks, security, uncover

6 An authentication-combined access control scheme using a geometric approach in distributed systems



Woei-Jiunn Tsaur, Shi-Jinn Horng, Chia-Ho Chen

April 1997 **Proceedings of the 1997 ACM symposium on Applied computing SAC '97**

Publisher: ACM Press

Full text available:  pdf(498.43 KB) Additional Information: [full citation](#), [references](#), [index terms](#)

Keywords: access control, cryptography, distributed systems, user authentication


7 Role-based access control on the web



Joon S. Park, Ravi Sandhu, Gail-Joon Ahn

February 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 1

Publisher: ACM Press

Full text available:  [pdf\(331.03 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

Current approaches to access control on the Web servers do not scale to enterprise-wide systems because they are mostly based on individual user identities. Hence we were motivated by the need to manage and enforce the strong and efficient RBAC access control technology in large-scale Web environments. To satisfy this requirement, we identify two different architectures for RBAC on the Web, called user-pull and server-pull. To demonstrate feasibility, we im ...

Keywords: WWW security, cookies, digital certificates, role-based access control

8 Secure authentication system for public WLAN roaming

Ana Sanz Merino, Yasuhiko Matsunaga, Manish Shah, Takashi Suzuki, Randy H. Katz
June 2005 **Mobile Networks and Applications**, Volume 10 Issue 3


Publisher: Kluwer Academic Publishers

Full text available:  [pdf\(2.43 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

A serious challenge for seamless roaming between independent wireless LANs (WLANs) is how best to confederate the various WLAN service providers, each having different trust relationships with individuals and each supporting their own authentication schemes, which may vary from one provider to the next. We have designed and implemented a comprehensive single sign-on (SSO) authentication architecture that confederates WLAN service providers through trusted identity providers. Users select the app ...

Keywords: authentication, link layer security, policy control, roaming, wireless LAN

9 Services: Secure authentication system for public WLAN roaming

 Yasuhiko Matsunaga, Ana Sanz Merino, Takashi Suzuki, Randy H. Katz
September 2003 **Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots WMASH '03**


Publisher: ACM Press

Full text available:  [pdf\(248.60 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

A serious impediment for seamless roaming between independent wireless LANs (WLANs) is how best to confederate the various WLAN service providers, each having different trust relationships with individuals and each supporting their own authentication schemes which may vary from one provider to the next. We have designed and implemented a comprehensive single sign-on (SSO) authentication architecture that confederates WLAN service providers through trusted identity providers. Users select the app ...

Keywords: authentication, hotspot, link layer security, policy control, roaming, single sign-on, wireless LAN

10 Unlinkable serial transactions: protocols and applications

 Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4

Publisher: ACM Press

Full text available:  [pdf\(184.87 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable

subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

Keywords: anonymity, blinding, cryptographic protocols, unlinkable serial transactions

11 Data Security



Dorothy E. Denning, Peter J. Denning
September 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 3

Publisher: ACM Press

Full text available: pdf(1.97 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

12 A secure and private system for subscription-based remote services



Pino Persiano, Ivan Visconti
November 2003 **ACM Transactions on Information and System Security (TISSEC)**,
Volume 6 Issue 4

Publisher: ACM Press

Full text available: pdf(241.65 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

In this paper we study privacy issues regarding the use of the SSL/TLS protocol and X.509 certificates. Our main attention is placed on subscription-based remote services (e.g., subscription to newspapers and databases) where the service manager charges a flat fee for a period of time independent of the actual number of times the service is requested. We start by pointing out that restricting the access to such services by using X.509 certificates and the SSL/TLS protocol, while preserving the in ...

Keywords: Access control, anonymity, cryptographic algorithms and protocols, privacy, world-wide web

13 Integrating security in a large distributed system



M. Satyanarayanan
August 1989 **ACM Transactions on Computer Systems (TOCS)**, Volume 7 Issue 3

Publisher: ACM Press

Full text available: pdf(2.90 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

Andrew is a distributed computing environment that is a synthesis of the personal computing and timesharing paradigms. When mature, it is expected to encompass over 5,000 workstations spanning the Carnegie Mellon University campus. This paper examines the security issues that arise in such an environment and describes the mechanisms that have been developed to address them. These mechanisms include the logical and physical separation of servers and clients, support for secure communication ...

14 Mobility support and location awareness: An approach to enhance inter-provider roaming through secret sharing and its application to WLANs



Ulrike Meyer, Jared Cordasco, Susanne Wetzel
September 2005 **Proceedings of the 3rd ACM international workshop on Wireless mobile applications and services on WLAN hotspots WMASH '05**

Publisher: ACM Press

Full text available: pdf(278.20 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

In this paper, we show how secret sharing can be used to address a number of shortcomings in state-of-the-art public-key-based inter-provider roaming. In particular, the new concept does not require costly operations for certificate validation by the mobile device. It furthermore eliminates the need for a secure channel between providers upon roaming. We demonstrate the new approach by introducing a new protocol, EAP-TLS-KS, for roaming between 802.11i-protected WLANs. In addition, we show that ...

Keywords: 802.11i, EAP-TLS-KS, PKI, WLAN, distributed DSS, inter-provider roaming, micropayment scheme, secret sharing

15 Applications, services, and architecture: Smart edge server: beyond a wireless access point



G. Manjunath, T. Simunic, V. Krishnan, J. Tourrilhes, D. Das, V. Srinivasmurthy, A. McReynolds

October 2004 **Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots WMASH '04**

Publisher: ACM Press

Full text available: pdf(410.68 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Wireless access at cafes, airports, homes and businesses have proliferated all over the globe with several different Wireless Internet Service Providers. Similarly, digital media has created a paradigm shift in media processing resulting in a complete change in media usage models, revamped existing businesses and has introduced new industry players. We believe there is a tremendous opportunity for application and system services at the intersection of the above two domains for exploiting the ...

Keywords: access point, low-power, management, media, security, wireless

16 Security: Zero-interaction authentication



Mark D. Corner, Brian D. Noble

September 2002 **Proceedings of the 8th annual international conference on Mobile computing and networking MobiCom '02**

Publisher: ACM Press

Full text available: pdf(273.30 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Laptops are vulnerable to theft, greatly increasing the likelihood of exposing sensitive files. Unfortunately, storing data in a cryptographic file system does not fully address this problem. Such systems ask the user to imbue them with long-term authority for decryption, but that authority can be used by anyone who physically possesses the machine. Forcing the user to frequently reestablish his identity is intrusive, encouraging him to disable encryption. Our solution to this problem is Zero- ...

Keywords: *cryptographic file systems, mobile computing, stackable file systems, transient authentication*

17 Secure password-based cipher suite for TLS



May 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 2

Publisher: ACM Press

Full text available: pdf(507.57 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

SSL is the de facto standard today for securing end-to-end transport on the Internet. While the protocol itself seems rather secure, there are a number of risks that lurk in its

use, for example, in web banking. However, the adoption of password-based key-exchange protocols can overcome some of these problems. We propose the integration of such a protocol (DH-EKE) in the TLS protocol, the standardization of SSL by IETF. The resulting protocol provides secure mutual authentication and key establi ...

Keywords: Authenticated key exchange, dictionary attack, key agreement, password, perfect forward secrecy, secure channel, transport layer security, weak secret

18 Access management for distributed systems: Peer-to-peer access control



architecture using trusted computing technology

Ravi Sandhu, Xinwen Zhang

June 2005 **Proceedings of the tenth ACM symposium on Access control models and technologies SACMAT '05**

Publisher: ACM Press

Full text available: pdf(215.48 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citings](#), [index terms](#), [review](#)

It has been recognized for some time that software alone does not provide an adequate foundation for building a high-assurance trusted platform. The emergence of industry-standard trusted computing technologies promises a revolution in this respect by providing roots of trust upon which secure applications can be developed. These technologies offer a particularly attractive platform for security in peer-to-peer environments. In this paper we propose a trusted computing architecture to enforce ac ...

Keywords: access control, policy enforcement, security architecture, trusted computing

19 Authentication in office system internetworks



Jay E. Israel, Theodore A. Linden

July 1983 **ACM Transactions on Information Systems (TOIS)**, Volume 1 Issue 3

Publisher: ACM Press

Full text available: pdf(1.28 MB) Additional Information: [full citation](#), [references](#), [index terms](#)

20 Protecting applications with transient authentication



Mark D. Corner, Brian D. Noble

May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03**

Publisher: ACM Press

Full text available: pdf(294.40 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citings](#)

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)